

# On the Orbits of Solvable Linear Groups

Zoltán Halasi and Károly Podoski

## Abstract

Let  $G$  be a solvable linear group acting on the finite vectorpace  $V$  and assume that  $(|G|, |V|) = 1$ . In this paper we find  $x, y \in V$  such that  $C_G(x) \cap C_G(y) = 1$ . In particular, this answers a question of I. M. Isaacs. We complete some results of S. Dolphi, A. Seress and T. R. Wolf.

## 1 Introduction

One basic concept for computing with permutation groups is the notion of a base: For a permutation group  $G \leq \text{Sym}(\Omega)$  a set  $\{\omega_1, \omega_2, \dots, \omega_n\} \subseteq \Omega$  (or rather an ordered list) is called a base for  $G$  if only the identity fixes all of the elements of this set. There are a number of algorithms for permutation groups related to the concept of base, and these algorithms are faster if the size of the base is small. Hence it is useful to find small bases to permutation groups. Of course, we cannot expect a good result in general, since taking the natural action of  $S_n$ , the minimal size of a base is  $n - 1$ . On the other hand, there are a number of results if  $G$  is solvable, the action of  $G$  is primitive, or  $(|G|, |\Omega|) = 1$ .

A size of a base of a permutation group  $G \leq \text{Sym}(\Omega)$  is at least  $\log |G| / \log |\Omega|$ . It is a conjecture of L. Pyber [10] that for a primitive permutation group  $G$  there is a base of size less than  $C \log |G| / \log |\Omega|$  for some universal constant  $C$ . For solvable groups, there is a more general result: It was proved by A. Seress [11] that all primitive solvable permutation group has a base of size at most four. According to the O’Nan–Scott Theorem, any such group is of affine type. However, in general there is no universal upper bound on the minimal base size of an affine group.

The situation changes, if we consider coprime affine groups. A permutation group  $G \leq \text{Sym} \Omega$  is said coprime, if  $(|G|, |\Omega|) = 1$ . It turns out that for coprime affine groups there is an upper bound for the minimal base size: It was proved by D. Gluck K. Magaard [4] that any such group has a base of size at most. As the result of Seress is sharp, the value of 95 can probably be improved.

Maybe the most examined case when  $V$  is a finite vector space,  $G \leq GL(V)$  is a solvable linear group and  $(|G|, |V|) = 1$ . It was asked by I. M. Isaacs [6] whether there always exists a  $G$ -orbit in  $V$  of size at least  $|G|^{1/2}$  for such groups. This follows immediately if we find  $x, y \in V$  such that  $C_G(x) \cap C_G(y) = 1$ , that is, a base of size two. The existence of such vectors was confirmed by T. R. Wolf [13] in case of  $G$  is supersolvable. Later, in a common work with A. Moretó [8] they solved this problem in case  $|G|$  and  $|V|$  are both odd. And S. Dolphi [1] proved that it is enough to assume that  $G$  is odd.

The goal of this paper is to prove the following theorem, which completes the remaining cases clear.

**Theorem 1.1.** *Let  $V$  be finite vector space over the field of size  $p$ , where  $p \neq 2$  is a prime, and let  $G \leq GL(V)$  be a solvable linear group with the assumption  $(|G|, |V|) = 1$ . Then there exist  $x, y \in V$  such that  $C_G(x) \cap C_G(y) = 1$ .*

Using Hartley–Turull Lemma [5] this yields

**Theorem 1.2.** *Let  $G$  be a finite group acting faithfully on a finite group  $K$  such that  $(|G|, |K|) = 1$ . Then there exist  $x, y \in K$  such that  $C_G(x) \cap C_G(y) = 1$ .*

## 2 Regular partitions for solvable permutation groups

Throughout this section let  $\Omega$  be a finite set and let  $G \leq \text{Sym}(\Omega)$  be a solvable permutation group. For a subset  $X \subseteq \Omega$  let  $G(X)$  denote the set-wise stabilizer of  $X$  in  $G$ -ben, that is,  $G(X) = \{g \in G \mid gx \in X \text{ for all } x \in X\}$ . We say that the partition  $\{\Omega_1, \Omega_2, \dots, \Omega_k\}$  of  $\Omega$  is  $G$ -regular, if only the identity element of  $G$  fixes all elements of this partition, i.e., if  $\cap_{i=1}^k G(\Omega_i) = 1$ .

With the additional assumption that  $G$  is a  $p'$ -group, one goal of this section is to show a  $G$ -regular partition of  $\Omega$  to at most  $p$  parts. Such a partition will be used in section 4 to reduce the problem to primitive linear groups. Moreover, our constructions for primitive permutation groups will be useful even in the discussion of the primitive linear case. Since a primitive solvable permutation group is of affine type, first we construct such partitions for affine groups.

**Theorem 2.1.** *Let  $W$  be an  $n$  dimensional vectorspace over the  $q$ -element field ( $q$  is prime), and let  $AGL(W)$  denote the full affine group acting on  $W$ . Furthermore, let  $G = W \rtimes G_0 \leq AGL(W)$  be any subgroup. If  $\{\underline{e}_1, \underline{e}_2, \dots, \underline{e}_n\}$  is a basis of  $W$ , then, depending on  $n$  and  $q$ , the following partitions are  $G$ -regular.*

*Case 1:  $|W| \leq 4$*

*Take the trivial partition, that is, each element of the partition consists of a single element.*

*Case 2:  $n = 1, q \geq 5$*

$$\Omega_1 = \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = V \setminus (\Omega_1 \cup \Omega_2).$$

*Case 3:  $n \geq 2, q \geq 5$*

$$\begin{aligned} \Omega_1 &= \{\underline{0}\}, \\ \Omega_2 &= \{\underline{e}_1, 2\underline{e}_1, \underline{e}_2, \underline{e}_3, \dots, \underline{e}_n, \underline{e}_1 + \underline{e}_2, \underline{e}_2 + \underline{e}_3, \dots, \underline{e}_{n-1} + \underline{e}_n\}, \\ \Omega_3 &= V \setminus (\Omega_1 \cup \Omega_2). \end{aligned}$$

*Case 4:  $n \geq 2, q = 3$*

$$\begin{aligned} \Omega_1 &= \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = \{\underline{e}_2, \underline{e}_3, \dots, \underline{e}_n, \underline{e}_1 + \underline{e}_2, \underline{e}_2 + \underline{e}_3, \dots, \underline{e}_{n-1} + \underline{e}_n\}, \\ \Omega_4 &= V \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3). \end{aligned}$$

*Case 5:  $n = 3, q = 2$*

$$\begin{aligned} \Omega_1 &= \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = \{\underline{e}_2\}, \quad \Omega_4 = \{\underline{e}_3\}, \\ \Omega_5 &= V \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4). \end{aligned}$$

Case 6:  $n \geq 4$ ,  $q = 2$

$$\begin{aligned}\Omega_1 &= \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = \{\underline{e}_2\}, \\ \Omega_4 &= \{\underline{e}_3, \dots, \underline{e}_n, \underline{e}_3 + \underline{e}_4, \underline{e}_4 + \underline{e}_5, \dots, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_3 + \underline{e}_2, \underline{e}_n + \underline{e}_1\}, \\ \Omega_5 &= V \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4).\end{aligned}$$

Case 7:  $n = 2$ ,  $q = 2$ , and the order of  $|G|$  is not divisible by 3

Let  $\Omega_1 = \{\underline{0}\}$ . The action of  $G(\Omega_1)$  on  $V \setminus \Omega_1 = \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + \underline{e}_2\}$  cannot be transitive, so it has a fix point in  $V \setminus \Omega_1$ , say,  $\underline{e}_1$ . Then

$$\Omega_1 = \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_2\}, \quad \Omega_3 = V \setminus (\Omega_1 \cup \Omega_2).$$

is  $G$ -regular.

Case 8:  $n = 3$ ,  $q = 2$ , and the order of  $|G|$  is not divisible by 3

Let  $\Omega_1 = \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + \underline{e}_2\}$ . The action of  $G(\Omega_1)$  on  $\Omega_1$  cannot be transitive, so it has a fix point in  $\Omega_1$ , say,  $\underline{e}_1$ .

If  $|G_0|$  is not divisible by 4, then there exists an  $\underline{x} \in V \setminus (\Omega_1 \cup \{\underline{0}\})$ , such that

$$\Omega_1 = \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + \underline{e}_2\}, \quad \Omega_2 = \{\underline{0}, \underline{x}\}, \quad \Omega_3 = V \setminus (\Omega_1 \cup \Omega_2).$$

is  $G$ -regular.

Otherwise, we can assume that  $G_0$  is contained in the group of upper unitriangular matrices. In this case

$$\Omega_1 = \{\underline{e}_1, \underline{e}_3, \underline{e}_1 + \underline{e}_3\}, \quad \Omega_2 = \{\underline{e}_2, \underline{e}_2 + \underline{e}_3\}, \quad \Omega_3 = V \setminus (\Omega_1 \cup \Omega_2).$$

is  $G$ -regular.

Case 9:  $n \geq 4$ ,  $q = 2$ , and the order of  $|G|$  is not divisible by 3

Let  $\Omega_1 = \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + \underline{e}_2\}$ . The action of  $G(\Omega_1)$  on  $\Omega_1$  cannot be transitive, so it has a fix point in  $\Omega_1$ , say,  $\underline{e}_1$ . Then the following partition is  $G$ -regular.

$$\begin{aligned}\Omega_1 &= \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + \underline{e}_2\}, \\ \Omega_2 &= \{\underline{e}_3, \underline{e}_4, \dots, \underline{e}_n, \underline{e}_3 + \underline{e}_4, \dots, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_3 + \underline{e}_2, \underline{e}_n + \underline{e}_1\}, \\ \Omega_3 &= V \setminus (\Omega_1 \cup \Omega_2).\end{aligned}$$

*Proof.* We show the  $G$ -regularity of the given partition only in Case 9. In the remaining cases one can prove the same by using similar but simpler arguments.

Our first observation is that  $G(\Omega_1)$  fixes  $\underline{0}$ , since  $\Omega_1 \cup \{\underline{0}\}$  is the only 2-dimensional affine subspace containing  $\Omega_1$ . Hence  $G(\Omega_1) \leq GL(W)$ . Let  $g \in G(\Omega_1) \cap G(\Omega_2)$ . We claim that  $g(\underline{e}_i) = \underline{e}_i$  for all  $1 \leq i \leq n$ -re, that is,  $g = 1$ . First,  $g(\underline{e}_2) = \underline{e}_2$  or  $g(\underline{e}_2) = \underline{e}_1 + \underline{e}_2$  by our assumption to  $\underline{e}_1$ . In the second case  $g(\underline{e}_3) \in \Omega_2$  and  $g(\underline{e}_2 + \underline{e}_3) = \underline{e}_1 + \underline{e}_2 + g(\underline{e}_3) \in \Omega_2$ . It is easy to check that there is no  $\underline{x} \in \Omega_2$  such that  $\underline{e}_1 + \underline{e}_2 + \underline{x} \in \Omega_2$ . (Here we need  $n \geq 4$ ). So  $g(\underline{e}_2) = (\underline{e}_2)$ .

To prove that  $g(\underline{e}_k) = \underline{e}_k$  for all  $3 \leq k < n$  we use induction to  $k$ . Assuming that  $g(\underline{e}_i) = \underline{e}_i$  for all  $1 \leq i < k < n$ , it follows that  $g(\underline{e}_k)$  and  $g(\underline{e}_{k-1} + \underline{e}_k)$  are elements of the set

$$\Omega_2 \setminus \langle \underline{e}_1, \dots, \underline{e}_{k-1} \rangle = \{\underline{e}_k, \underline{e}_{k+1}, \dots, \underline{e}_n, \underline{e}_{k-1} + \underline{e}_k, \dots, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_n + \underline{e}_2\}.$$

Since  $g(\underline{e}_k) + g(\underline{e}_{k-1} + \underline{e}_k) = \underline{e}_{k-1}$ , we have either  $g(\underline{e}_k)$  or  $g(\underline{e}_{k-1} + \underline{e}_k)$  contains  $\underline{e}_{k-1}$  with non-zero coefficient. However, the only such element in the set  $\Omega_2 \setminus \langle \underline{e}_1, \dots, \underline{e}_{k-1} \rangle$  is  $\underline{e}_{k-1} + \underline{e}_k$ . So either  $g(\underline{e}_{k-1} + \underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$  or  $g(\underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$ . In the latter case  $\underline{e}_k + \underline{e}_{k+1} \in \Omega_2$ , since  $k < n$ , but  $g(\underline{e}_k + \underline{e}_{k+1}) \notin \Omega_2$ , a contradiction. It follows that  $g(\underline{e}_{k-1} + \underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$ , which proves that  $g(\underline{e}_k) = \underline{e}_k$ . It remains to prove that  $g(\underline{e}_n) = \underline{e}_n$ . It is clear that

$$g(\underline{e}_n) \in \Omega_2 \setminus \langle \underline{e}_1, \underline{e}_2, \dots, \underline{e}_{n-1} \rangle = \{\underline{e}_n, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_n + \underline{e}_1\}.$$

If  $g(\underline{e}_n) = \underline{e}_{n-1} + \underline{e}_n$ , then  $g(\underline{e}_n + \underline{e}_1) = \underline{e}_{n-1} + \underline{e}_n + \underline{e}_1 \notin \Omega_2$ . If  $g(\underline{e}_n) = \underline{e}_n + \underline{e}_1$ , then  $g(\underline{e}_{n-1} + \underline{e}_n) = \underline{e}_{n-1} + \underline{e}_n + \underline{e}_1 \notin \Omega_2$ . Thus  $g(\underline{e}_n) = \underline{e}_n$  also holds. So  $G(\Omega_1) \cap G(\Omega_2) = 1$ , that is, the given partition is  $G$ -regular.  $\square$

These constructions have some properties, which will be important later. We summarize them in the following corollary.

**Corollary 2.2.** *If  $W \leq G \leq \text{AGL}(W)$  is an affine group,  $p \geq 3$  prime, and  $p$  does not divide the order of  $G$ , then there exists a  $G$ -regular partition of  $W$  into at most  $p$  parts. Moreover, this partition has the following properties.*

1. *In Case 1 the partition is trivial and it consists of at most  $p - 1$  parts. In any other case there is a part of “unique size”, that is, a part  $\Omega_i$  such that  $|\Omega_i| \neq |\Omega_j|$  if  $i \neq j$ .*
2. *Apart from a few exceptions, there is a “large” part. More precisely, the following inequalities holds:*

$$\begin{aligned} \text{In Case 2: } & |\Omega_2| = 1 < \frac{1}{4}|W|; \\ \text{In Case 3: } & |\Omega_2| = 2n < \frac{1}{4}5^n \leq \frac{1}{4}|W|; \\ \text{In Case 4: } & |\Omega_3| + 2 = 2n < \frac{1}{4}3^n = \frac{1}{4}|W|, \quad \text{if } n \geq 3; \\ \text{In Case 5: } & |\Omega_4| = 1 < \frac{1}{4}|W|; \\ \text{In Case 6: } & |\Omega_4| = 2n - 3 < \frac{1}{4}2^n = \frac{1}{4}|W|, \quad \text{if } n \geq 5. \end{aligned} \tag{1}$$

*So, one of the above inequalities holds, unless  $|W| = 2, 3, 4, 9$  or  $16$ .*

*Proof.* If  $W$  is a vector space over the  $q$ -element field, then  $(q, p) = 1$ , since  $G \geq W$ . Now, if  $p = 3$ , then  $q \neq 3$ , so one of the cases 1., 2., 3., 7., 8., or 9. holds, and in these cases the given partition is of 3 parts. If  $p \neq 3$ , then  $p \geq 5$ . Even in the remaining cases the given partition is of at most 5 parts. The remaining parts of the statement can be easily checked.  $\square$

Using the first part of this Corollary we can prove the existence of the wanted  $G$ -regular partition for any solvable  $p'$ -group.

**Theorem 2.3.** *Let  $G \leq \text{Sym}(\Omega)$  be a solvable permutation group, Assuming that the order of  $G$  is not divisible by  $p$ , there exists a  $G$ -regular partition of  $\Omega$  into at most  $p$  parts.*

Before proving this, first we give an alternative form of this statement, which will be easier to handle. Besides that, from this form it should be clearer what is the connection between finding  $G$ -regular partition for a permutation groups and finding a two-element base for a linear group. If  $\Omega = \{1, 2, \dots, n\}$ , then we have a natural inclusion  $\text{Sym}(\Omega) \rightarrow GL(n, p)$ . Hence  $\text{Sym}(\Omega)$  acts naturally

on  $\mathbb{F}_p^n$ . If we have a partition of  $\Omega$  into at most  $p$  parts, then we can color the elements of the partitions by the elements of  $\mathbb{F}_p$ , that is, there is an  $f : \Omega \rightarrow \mathbb{F}_p$  such that  $x, y \in \Omega$  are in the same part of the partition if and only if  $f(x) = f(y)$ . Thus, Theorem 2.3 is clearly equivalent to the following theorem.

**Theorem 2.4.** *If  $G$  is a solvable permutation group of degree  $n$ , and  $p$  does not divide the order of  $G$ , then there is an  $(a_1, a_2, \dots, a_n) \in \mathbb{F}_p^n$  vector, such that only the identity element of  $G$  fixes this vector.*

*Proof.* Although we do not deal with the case  $p = 2$ , we note that this follows from a Theorem of D. Gluck[3]. A direct short proof is given by H. Matsuyama [7]. Thus, let in the following  $p \geq 3$ .

If  $G$  is primitive permutation group, then Corollary 2.2 guarantees the existence of such a vector (or partition). In the following let  $G$  be a transitive, but not primitive group. Then there are blocks  $\Delta_i$ ,  $1 \leq i \leq k$ , such that  $1 < |\Delta_i| < |\Omega|$ ,  $\Omega = \Delta_1 \cup \Delta_2 \cup \dots \cup \Delta_k$  is a partition, and  $G$  permutes the  $\Delta_i$  sets transitively. We can assume that  $|\Delta_i|$  is as small as possible. Let  $H_i = G(\Delta_i)$  and  $N = \cap_{i=1}^k H_i$ . Now,  $G/N$  transitively on the set  $\tilde{\Omega} = \{\Delta_1, \Delta_2, \dots, \Delta_k\}$ . Using induction to  $|\tilde{\Omega}|$  we get a vector  $(a_1, a_2, \dots, a_k) \in \mathbb{F}_p^k$  such that only the identity element of  $G/N$  fixes this vector.

On the other hand,  $H_i/C_{H_i}(\Delta_i)$  acts primitively on  $\Delta_i$  for all  $1 \leq i \leq k$ , and these groups are all conjugate in  $G$ ; in particular, they are permutation isomorphic. Thus, for each  $i$  we can find a  $H_i/C_{H_i}(\Delta_i)$ -regular partition of  $\Delta_i$  by Corollary 2.2 and these partitions are essentially the same for  $1 \leq i \leq k$ .

If the first case holds in part 1 of the above Corollary, then  $|\Delta_i| \leq p - 1$ . In this case let us choose an  $A \subset \mathbb{F}_p$  subset such that  $|A| = |\Delta_i|$ , and let  $f_i : \Delta_i \rightarrow A + a_i = \{a + a_i \mid a \in A\}$  be a bijection for every  $1 \leq i \leq k$ .

If the second case holds in part 1 of the above Corollary, then for each  $i$  let us choose  $X_i \subseteq \Delta_i$  part of the partition of  $\Delta_i$ , such that it is of unique size. If there would be more than one such part, then we only need to pay attention that the size of each  $X_i$  must be the same. Now, let the function  $f_i : \Delta_i \rightarrow \mathbb{F}_p$  be defined as a coloring of the partition of  $\Delta_i$  such that  $f_i(X_i) = a_i$ .

Finally, let the function  $f : \Omega \rightarrow \mathbb{F}_p$  be defined as

$$f(x) = f_i(x), \quad \text{if } x \in \Delta_i.$$

The essence of this construction is that the distribution of  $f_i$  determines  $a_i$ . Hence, if  $g \in G$  fixes the vector  $(f(1), f(2), \dots, f(n)) \in \mathbb{F}_p^n$ , then  $gN$  fixes the vector  $(a_1, a_2, \dots, a_k) \in \mathbb{F}_p^k$ , so  $g \in N$  and  $g(\Delta_i) = \Delta_i$  for each  $1 \leq i \leq k$ . Finally, from the construction of the  $f_i$ -s we get  $g \in \cap_{i=1}^k C_{H_i}(\Delta_i) = 1$ .  $\square$

### Remark

It was proven by Á. Seress [11, Theorem 1.2.] that for any  $G \leq \text{Sym}(\Omega)$  solvable permutation group there always exists a  $G$ -regular partition of  $\Omega$  into at most five parts.

Our last result concerning permutation groups is showing regular partitions to groups of affine type with “mixed characteristic”. This will play a role in the discussion of primitive linear groups.

**Theorem 2.5.** *For each  $1 \leq i \leq k$  let  $W_i$  be a finite vector space over the  $p_i$ -element field, where  $p_1 < p_2 < \dots < p_k$  and  $k \geq 2$ . Furthermore, let  $\bigoplus_{i=1}^k W_i \leq G \leq \text{AGL}(W_1) \times \text{AGL}(W_2) \times \dots \times \text{AGL}(W_k)$  acting on  $W = W_1 \oplus W_2 \oplus \dots \oplus W_k$  in the natural way. Then there exists a  $G$ -regular  $W = \Omega_1 \cup \Omega_2 \cup \Omega_3$  partition such that  $\Omega_1 = \{\underline{0}\}$  and  $|\Omega_2| < \frac{1}{4}|W|$ .*

*Proof.* For each  $1 \leq i \leq k$  let  $\underline{e}_{i,1}, \underline{e}_{i,2}, \dots, \underline{e}_{i,n_i}$  be a basis of  $W_i$ , where  $n_i = \dim W_i$ . To show a suitable  $\Omega_2$  we use the cases 1-6 of Theorem 2.1. We saw that there are  $\Omega_i^* \subseteq W_i$  subsets such that  $G(\underline{0}) \cap G(\Omega_i^*) = 1$  for  $p_i \geq 5$ , or  $|W_i| \leq 3$ ,  $G(\underline{0}) \cap G(\Omega_i^*) \cap G(\underline{e}_{i,1}) = 1$  for  $p_i = 3$  or  $|W_i| = 4$  and  $G(\underline{0}) \cap G(\Omega_i^*) \cap G(\underline{e}_{i,1}) \cap G(\underline{e}_{i,2}) = 1$  for  $p_i = 2, n_i \geq 3$ . Now, let  $\Omega_2$  be defined as

$$\begin{cases} \{\underline{e}_{1,1} + \underline{e}_{2,1}, \underline{e}_{1,1} + 2\underline{e}_{2,1}, \underline{e}_{1,2} + \underline{e}_{2,1}\} \cup \Omega_1^* \cup \Omega_2^* \cup \dots \cup \Omega_k^*, & \text{if } p_1 = 2, n_1 \geq 3; \\ \{\underline{e}_{1,1} + \underline{e}_{2,1}\} \cup \Omega_1^* \cup \Omega_2^* \cup \dots \cup \Omega_k^*, & \text{otherwise.} \end{cases}$$

Now,  $G(\underline{0})$  is a subgroup of the automorphism group of  $\bigoplus W_i$ , so it fixes each  $W_i$ . Thus, if  $g \in G(\underline{0}) \cap G(\Omega_2)$ , then  $g$  fixes each  $W_i \cap \Omega_2 = \Omega_i^*$ , and it permutes the three (or one) exceptional elements. Using that  $g(\underline{e}_{1,1}), g(\underline{e}_{1,2}) \in W_1$ ,  $g(\underline{e}_{2,1}) \in W_2$ , we get  $g$  fixes also these elements. Hence  $g$  acts trivially on every  $W_i$ , so  $g = 1$ , and we found a  $G$ -regular partition.

Let  $l = n_1 + \dots + n_k$ . Then  $|W| \geq 2^{l-1}3$ , since  $k \geq 2$ . We saw that  $|\Omega_i^*| \leq 2n_i$ , and  $|\Omega_1^*| \leq 2n_1 - 3$ , if  $p_1 = 2$ ,  $n_1 \geq 3$ . It follows that  $|\Omega_2| \leq 1 + 2l < \frac{1}{4}2^{l-1}3 \leq \frac{1}{4}|W|$  holds, unless  $l \leq 4$ . Now, assume that  $l \leq 4$ . If each  $n_i \leq 2$ , then let  $\Omega_2 = \{\sum_i \underline{e}_{i,1}\} \cup \{\underline{e}_{j,2} \mid n_j = 2\}$ , which is clearly  $G(\underline{0})$ -regular, and for which  $|\Omega_2| = l - 1 < \frac{1}{4}2^{l-1}3 \leq 1/4|W|$  holds. In case of  $n_1 = 3$ ,  $p_1 = 2$ ,  $n_2 = 1$ , we have  $|\Omega_1^*| = |\Omega_2^*| = 1$ , so  $|\Omega_2| = 3 + 1 + 1 < \frac{1}{4}2^33 \leq \frac{1}{4}|W|$ . Finally, if  $|W| = p^3q$  for some  $p \neq 2, q$  primes, then  $|\Omega_2| \leq 1 + 6 \leq \frac{1}{4}3^32 \leq \frac{1}{4}|W|$ .  $\square$

### 3 Primitive linear groups

In the following let  $V \simeq \mathbb{F}_p^n$  be a finite vector space and let  $G \leq GL(V) \simeq GL(n, p)$  be a solvable linear group such that  $(|G|, p) = 1$ . In this section we assume that  $G$  is a primitive linear group, that is, there does not exist a

$$V = V_1 \oplus V_2 \oplus \dots \oplus V_t$$

proper decomposition of  $V$ , such that  $G$  permutes the  $V_i$  subspaces. (We deal with imprimitive linear groups in section 4.) In order to find vectors  $x, y \in V$  such that  $C_G(x) \cap C_G(y) = 1$ , we can clearly assume that  $G$  is maximal (with respect to inclusion) among the solvable  $p'$ -subgroups of  $GL(V)$ . The main idea of our construction is the following: Using that the Fitting subgroup of  $G$  (denoted by  $F$ ) has a very special structure, we show the existence of a basis of  $V$  such that every element of  $F$  is “almost” monomial in this basis. Next, we choose  $x$  in such a way that  $C_G(x)$  is also “almost” monomial subgroup in this basis. Now, the permutation part of  $F$  defines a linear space on this special basis, and the permutation part of  $C_G(x)$  acts on this space as a linear group. Hence we can use the constructions given in Theorem 2.1 and in Theorem 2.5 to find a suitable  $y$ .

### 3.1 The structure of the Fitting subgroup

If  $G \leq GL(V)$  is a maximal solvable  $p'$ -subgroup, then it is a  $p'$ -Hall subgroup of some  $H \leq GL(V)$  maximal solvable subgroup. Some relevant properties of such groups can be found in [9, Proposition 2.1], [11, Lemma 2.2] and in [12, §19–20]. We collect them in the following theorem.

**Theorem 3.1.** *Let  $H \leq GL(n, p)$  be a maximal solvable primitive group. Then  $H$  contains a unique maximal abelian normal subgroup, denoted by  $A$ . Furthermore, let  $C = C_H(A)$  and  $F = \text{Fit}(C)$ , the Fitting subgroup of  $C$ . Now,  $A \leq F \leq C \leq H$  are all normal subgroups of  $H$ , which have the following properties.*

1.  $A$  is cyclic and  $|A| = p^a - 1$  for some  $a$ .
2. The linear span of  $A$  is isomorphic to the field  $\mathbb{F}_{p^a}$ .
3. The action of  $H/C$  on  $A$  gives us an inclusion  $H/C \hookrightarrow \mathbb{F}_{p^a}^*$ .
4.  $F = AP_1P_2 \dots P_k$ , where  $P_i$  is an extraspecial  $p_i$ -group of order  $p_i^{2e_i+1}$  for each  $i$ . Furthermore,  $Z(P_i) = A \cap P_i$ , and  $A$  contains all the  $p_i$ -th roots of unity. If  $p_i > 2$ , then the exponent of  $P_i$  is  $p_i$ .
5. Let  $e = \prod p_i^{e_i}$ . Then  $n = ea$ .
6.  $C$  is included in  $GL(e, p^a)$ .
7.  $F \leq GL(e, p^a)$  gives an irreducible representation of  $F$ .

Now, if  $G \leq H$  is a  $p'$ -Hall subgroup of  $H$ , then we claim that  $A \leq F \leq G$ . Indeed,  $A$  and  $F$  both are normal  $p'$ -subgroups of  $H$ , so they are contained in a  $p'$ -Hall subgroup of  $H$ . Since the  $p'$ -Hall subgroups are all conjugate, they are contained in  $G$ , too. Hence we can use the above theorem to  $G$ . By the next lemma we can assume that  $C_G(A) = G$ .

**Lemma 3.2.** *Let  $x, y \in V$  such that  $C_G(x) \cap C_G(y) = 1$ . Then for some  $\gamma \in A \cup \{0\} = \mathbb{F}_{p^a}$  we have  $C_G(x) \cap C_G(y + \gamma x) = 1$ .*

*Proof.* For any  $g \in G$  let  $\sigma_g \in \text{Aut}(\mathbb{F}_{p^a})$  denote the action of  $gC$  on  $\mathbb{F}_{p^a}$  by part 3 of Theorem 3.1. For all  $\alpha \in \mathbb{F}_{p^a}$  let the subgroup  $H_\alpha = C_G(x) \cap C_G(y + \alpha x) \leq G$ . Our aim is to prove that  $H_\alpha = 1$  for some  $\alpha \in \mathbb{F}_{p^a}$ .

Let  $g \in H_\alpha$ . Thus,  $g(x) = x$  and  $y + \alpha x = g(y + \alpha x) = g(y) + \alpha^{\sigma_g} x$ . Hence  $g(y) = y + (\alpha - \alpha^{\sigma_g})x$ . If  $g \in \langle \cup H_\alpha \rangle$ , then  $g$  is the product of elements from several  $H_\alpha$ 's. It follows that  $g(y) = y + \delta x$  for a  $\delta \in \mathbb{F}_{p^a}$ .

We claim that  $\langle \cup H_\alpha \rangle \cap C = 1$ . Let  $g \in \langle \cup H_\alpha \rangle_G \cap C$ . On the one hand, the action of  $g$  on  $V$  is  $\mathbb{F}_{p^a}$ -linear, since  $g \in C = C_G(A)$ . On the other hand,  $g(x) = x$  and  $g(y) = y + \delta x$  for a  $\delta \in \mathbb{F}_{p^a}$  by the previous part. If  $g^n = 1$ , then  $y = g^n(y) = y + n\delta x$ , so  $n\delta = 0$ . Using that  $|G|$  is coprime to  $p$ , we get  $n$  is not divisible by  $p$ , hence  $\delta = 0$ . Therefore,  $g(y) = y$  and  $g \in C_G(x) \cap C_G(y) = 1$ .

Since  $G/C \leq \text{Aut}(\mathbb{F}_{p^a})$ , for any  $g \neq h \in \cup H_\alpha$  we have  $\sigma_g \neq \sigma_h$ . Furthermore, the subfields of  $\mathbb{F}_{p^a}$  fixed by  $\sigma_g$  and  $\sigma_h$  are the same if and only if  $\langle g \rangle_G = \langle h \rangle_G$ . If  $g \in H_\alpha \cap H_\beta$ , then  $g(y) = y + (\alpha - \alpha^{\sigma_g})x = y + (\beta - \beta^{\sigma_g})x$ , so  $\alpha - \beta$  is fixed by  $\sigma_g$ .

Let  $K_g = \{\alpha \in \mathbb{F}_{p^a} \mid g \in H_\alpha\}$ . The previous calculation shows that  $K_g$  is an

additive coset of the subfield fixed by  $\sigma_g$ , so  $|K_g| = p^d$  for some  $d|a$ . Since for any  $d|a$  there is a unique  $p^d$ -element subfield of  $\mathbb{F}_{p^a}$ , we get  $|K_g| \neq |K_h|$  unless the subfields fixed by  $\sigma_g$  and  $\sigma_h$  are the same. As we have seen, this means  $\langle g \rangle_G = \langle h \rangle_G$ . Consequently,  $|K_g| \neq |K_h|$  unless  $K_g = K_h$ . Hence we get the following

$$\left| \bigcup_{g \in \cup H_\alpha \setminus \{1\}} K_g \right| \leq \sum_{d|a, d < a} p^d \leq \sum_{d < a} p^d = \frac{p^a - 1}{p - 1} < p^a.$$

So there is a  $\gamma \in \mathbb{F}_{p^a}$  which is not contained in  $K_g$  for any  $g \in \cup H_\alpha \setminus \{1\}$ . This exactly means  $H_\gamma = C_G(x) \cap C_G(y + \gamma x) = 1$ .  $\square$

Henceforth, it is enough to find suitable  $x, y \in V \simeq \mathbb{F}_{p^a}^e$  vectors for such  $G \leq GL(e, p^a)$  solvable  $p'$ -groups, which have  $A \leq F \leq G$  normal subgroups,  $A$  consists of scalar matrices, and parts 4,5,7 of Theorem 3.1 holds to  $F$ . Observe that for each  $p \neq 2$  prime the 4th part of Theorem 3.1 determines the isomorphic type of the  $p$ -Sylow subgroup of  $F$ , since there are two types of extraspecial groups of order  $p^{2d+1}$  for any  $p$ : For  $p \neq 2$  one of them has exponent  $p$ , the other one has exponent  $p^2$ . However, for  $p = 2$  both of them has exponent 4. In this case one of them is the central product of  $d$  copies of dieder groups  $D_4$ , the other one is the central product of a quaternion group  $Q$  and  $d - 1$  copies of  $D_4$ . This gives us two possible isomorphism type to  $F$ . We say that  $F$  is monomial, if in the above decomposition of  $F$  either each  $p_i \neq 2$  (that is,  $e$  is odd), or the occuring extraspecial subgroup in  $F$ , say  $P_1$ , is a central power of  $D_4$ . Otherwise, we say that  $F$  is not monomial. (The explanation of our term “monomial” is that in the first case we can choose a basis such that written in this basis every element of  $F$  will be monomial matrix.)

### 3.2 Finding $x, y \in V$ in case $F$ is monomial

Let in the following  $F \triangleleft G \leq GL(V) \simeq GL(e, p^a)$ , where  $F$  monomial, that is, the extraspecial subgroup of  $F$  occuring in part 4 of Theorem 3.1 is a central power of  $D_4$  (maybe trivial). The next theorem help us to find a “good” basis to  $F$ .

**Theorem 3.3.** *With the above assumptions the following hold to  $F \triangleleft GL(V)$ :*

1. *There is a decomposition  $F = D \rtimes S$  such that  $D = A \times D_0$ , and*

$$D_0 \simeq S \simeq Z_{p_1}^{e_1} \times Z_{p_2}^{e_2} \times \dots \times Z_{p_k}^{e_k}.$$

2. *There is a basis  $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e \in V$  such that written in this basis  $D$  consists of diagonal matrices and  $S$  regularly permutes the elements of this basis.*
3. *The subspaces  $\langle \underline{u}_i \rangle$ ,  $1 \leq i \leq e$  are all the irreducible representations of  $D_0$  over  $\mathbb{F}_{p^a}$ , and they are pairwise non-equivalent.*
4. *If  $g \in D_0$ , then  $g$  contains all of the  $o(g)$ -th roots of the unity with the same multiplicity.*

*Proof.* It is well-known that any extraspecial  $p$ -group is the central product of non-abelian groups of order  $p^3$ . Taking our restriction to  $P_i$  in to account in case  $p_i = 2$  and using that the exponent of  $P_i$  is  $p_i$  for  $p_i > 2$  we can find generators

$$P_i = \langle x_{i,1}, x_{i,2}, \dots, x_{i,e_i}, y_{i,1}, y_{i,2}, \dots, y_{i,e_i}, z_i \rangle,$$



such that any generator is of order  $p_i$ ,  $Z(P_i) = \langle z_i \rangle$ , and  $[x_{i,l}, y_{i,l}] = z_i$  for all  $1 \leq l \leq e_i$ , any other pair of generators are commuting. Now, let  $D_i = \langle x_{i,1}, x_{i,2}, \dots, x_{i,e_i} \rangle$ , and  $S_i = \langle y_{i,1}, y_{i,2}, \dots, y_{i,e_i} \rangle$ . Finally, let

$$D = A \times D_1 \times D_2 \times \dots \times D_k \quad \text{és} \quad S = S_1 \times S_2 \times \dots \times S_k.$$

Now, it should be clear that the decomposition  $F = D \rtimes S$  fulfill the requirement 1. (Although we did not fix  $D_0$ -t yet!) Using part 4 of Theorem 3.1, we get  $A = \mathbb{F}_{p^a}^*$  contains all of the  $\exp(D)$ -th roots of unity, hence every irreducible representation of  $D$  over  $\mathbb{F}_{p^a}$  is one dimensional. Fix an  $\underline{u}_1 \in V$  in such a way that  $\mathbb{F}_{p^a} \underline{u}_1$  is a  $D$ -invariant subspace. Choosing  $D_0 = C_D(\underline{u}_1)$  we have  $D = A \times D_0$ .

Now, let the basis  $\{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e\}$  be defined as the set  $\{s(\underline{u}_1) \mid s \in S\}$ . First of all,  $e = |S| = \dim V$ . As  $D \triangleleft F$ , it follows that  $Ds(\underline{u}_1) = sD(\underline{u}_1)$ , so  $\mathbb{F}_{p^a} s\underline{u}_1$  is also a  $D$ -invariant subspace for all  $s \in S$ . Hence  $\langle \underline{u}_1, \underline{u}_2, \dots, \underline{u}_e \rangle$  is an  $F = DS$ -invariant subspace, so it is equal to  $V$  by part 7 of Theorem 3.1. Therefore,  $\{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e\}$  is indeed a basis of  $V$ . From our construction 2 clearly follows. The 3rd part of the statement follows easily from the fact  $C_S(D_0) = 1$ . Let  $\underline{u}_i = s(\underline{u}_j)$ , where  $1 \neq s \in S$ . Furthermore, let  $d \in D_0$  such that the scalar matrix  $[d, s] \neq 1$ . Then

$$d_{jj}\underline{u}_j = d(\underline{u}_j) = ds(\underline{u}_i) = sd[d, s](\underline{u}_i) = [d, s](d_{ii}\underline{u}_j),$$

so  $d_{jj} \neq d_{ii}$ , which proves that these representations are pairwise non-isomorphic. The statement that these representations give us all the irreducible representations of  $D_0$  follows from the fact  $|D_0| = e$ .

Finally, in view of the last statement, part 4 is just a special case of a more general statement to any  $A$  finite abelian group and to the groups of linear characters of  $A$  over  $K$  with the assumptions  $(|A|, |K|) = 1$  and  $K$  contains all of the  $\exp(A)$ -th roots of unity.  $\square$

In the following we fix a basis  $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e$ , which fulfill the requirements of the above theorem. With respect to this basis, we identify  $GL(V)$  with the matrix group  $GL(e, p^a)$ . Thus,  $F = DS \triangleleft G \leq GL(e, p^a)$ , where  $D$  is the group of diagonal matrices in  $F$  and  $S$  is the group of permutation matrices in  $F$  acting regularly on the selected basis. Furthermore,  $D = A \times D_0$ , where  $D_0 = C_D(\underline{u}_1) = C_F(\underline{u}_1)$ .

To find a base  $x, y \in V$  we write them as a linear combination of the matrices  $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e$  in such a way that  $x$  contains only a few (one or three)  $\underline{u}_i$  with non-zero coefficients, while  $y$  a lot of them.

Our next lemma collects some consequences of the choice  $x = \underline{u}_1$ :

**Lemma 3.4.** *Let  $g \in G$  be any group element fixing  $g(\underline{u}_1) = \underline{u}_1$ . Then*

1.  $D_0^g = D_0$ , and  $g$  is a monomial matrix. Hence there exists a  $g = \delta(g)\pi(g)$  decomposition of  $g$  to a diagonal matrix  $\delta(g)$  and to a permutation matrix  $\pi(g)$ .
2.  $\pi(g)$  normalizes  $S$ , that is,  $S^{\pi(g)} = S$ .
3. Both  $\delta(g)$  and  $\pi(g)$  normalize  $F$ , so  $F = F^{\delta(g)} = F^{\pi(g)}$ . Moreover,  $[\delta(g), S] \leq D$ .

4. If  $\delta(g) \neq 1$ , then the numbers of 1's in the main diagonal of  $\delta(g)$  is at most  $\frac{3}{4}e$ .

*Proof.* The statement  $D_0^g = D_0$  follows from the fact  $D_0 = C_F(\underline{u}_1) \triangleleft C_G(\underline{u}_1)$ . Consequently,  $g$  permutes the homogeneous components of the  $D_0$ -module  $V$ . By part 3 of Theorem 3.3, these homogeneous components are just the one-dimensional subspaces  $\langle \underline{u}_i \rangle$ ,  $1 \leq i \leq e$ . These means that  $g$  is a monomial matrix. Of course, a monomial matrix  $g$  has a unique decomposition  $g = \delta(g)\pi(g)$ , and part 1 is proved.

For any  $s \in S$  we have

$$s^g = \pi(g)^{-1}\delta(g)^{-1}s\delta(g)\pi(g) = \pi(g)^{-1}([\delta(g), s^{-1}]s)\pi(g) = [\delta(g), s^{-1}]^{\pi(g)}s^{\pi(g)}$$

is an element of  $F$ . The expression  $[\delta(g), s^{-1}]^{\pi(g)}$  on the right-hand side is diagonal, while  $s^{\pi(g)}$  is permutation matrix, so both of them are elements of  $F$ . However, any permutation matrix in  $F$  is contained in  $S$ , so  $s^{\pi(g)} \in S$ , and 2 follows.

Both  $g$  and  $\delta(g)$  normalize  $D$ , hence  $\pi(g) = \delta(g)^{-1}g$ , too. We have seen that  $\pi(g)$  normalizes  $S$ , so it normalizes also  $F = DS$ . We get  $\delta(g) = g\pi(g)^{-1}$  also normalizes  $F$ . Finally, the statement  $[\delta(g), S] \leq D$  follows from the fact that the commutator of a permutation matrix by a diagonal matrix is also diagonal. So 3 holds.

If  $\delta(g) \neq 1$ , then  $\delta(g)$  is not a scalar matrix, so there exists an  $s \in S$  such that  $[\delta(g), s] \neq 1$ . Now,  $[\delta(g), s] \in D \setminus \{1\}$ , so, using part 4 of Theorem 3.3, we get the number of 1's in the main diagonal of  $[\delta(g), s]$  is at most  $\frac{1}{2}e$ . This cannot be true if the number of 1's in  $\delta(g)$  is more than  $\frac{3}{4}e$ . We are done.  $\square$

We saw that for any  $g \in C_G(\underline{u}_1)$  there is a unique decomposition  $g = \delta(g)\pi(g)$ . The map  $\pi : g \rightarrow \pi(g)$  gives us a homomorphism from  $C_G(\underline{u}_1)$  into the group of permutation matrices.

By part 2 of Lemma 3.4 Lemma,  $\pi(C_G(\underline{u}_1))$  normalizes  $S$ , so it acts on  $S$  by conjugation, which defines a  $\pi(C_G(\underline{u}_1)) \rightarrow \text{Aut}(S)$  homomorphism. In fact, this homomorphism is an inclusion, since  $C_G(\underline{u}_1) \cap C_G(S) = 1$ . Therefore,  $\pi(C_G(\underline{u}_1)) \leq \text{Aut}(S) \simeq GL(e_1, p_1) \times GL(e_2, p_2) \times \cdots GL(e_k, p_k)$ .

This is usefull to us, because we can apply Theorems 2.1 and 2.5, to find a  $\pi(C_G(\underline{u}_1))$ -regular partition of  $S$ . Moreover, we do not need to fix the zero element of  $S$  (that is, the identity matrix); we already fixed it by choosing  $x = \underline{u}_1$ . Since  $S$  acts on the basis  $W = \{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e\}$  regularly, using the bijection  $s \rightarrow s(\underline{u}_1)$  we can define a partition  $W = \{\underline{u}_1\} \cup \Omega_2 \dots \cup \Omega_l$ , which is also  $\pi(C_G(\underline{u}_1))$ -regular.

### 3.2.1 Case $e \neq 2^t$

In the following we will assume that  $|D_0| = |S| = e$  is not a 2-power. In every such case let  $x = \underline{u}_1$ . By the last paragraph, we have a  $\pi(C_G(\underline{u}_1))$  regular partition  $W = \{\underline{u}_1\} \cup \Omega_2 \dots \cup \Omega_l$ . Let  $\alpha \in \mathbb{F}_{p^a}$  be a generator element of the multiplicative group of  $\mathbb{F}_{p^a}$ . Now,  $o(\alpha) = |A| \geq 6$ , since  $|A|$  is even ( $p \neq 2$ ) and every prime divisor of  $e$  divides  $|A|$ .

**Theorem 3.5.** *With the above notations let  $y$  be defined as follows*

$$\begin{aligned}
\text{For } e \neq 3^k : \quad & y = 0 \cdot \sum_{\underline{u}_i \in \Omega_2} \underline{u}_i + 1 \cdot \sum_{\underline{u}_i \in \Omega_3} \underline{u}_i, \\
\text{For } e = 3^k, \ k \geq 2 : \quad & y = \alpha \cdot \sum_{\underline{u}_i \in \Omega_2} \underline{u}_i + 0 \cdot \sum_{\underline{u}_i \in \Omega_3} \underline{u}_i + 1 \cdot \sum_{\underline{u}_i \in \Omega_4} \underline{u}_i, \\
\text{For } e = 3 : \quad & y = \alpha \underline{u}_2 + \underline{u}_3.
\end{aligned}$$

Then  $C_G(x) \cap C_G(y) = 1$ .

*Proof.* Let  $g \in C_G(x) \cap C_G(y)$ . Since  $g$  fixes  $\underline{u}_1 = x$ ,  $g$  is a monomial matrix by Lemma 3.4, so we have a decomposition  $g = \delta(g)\pi(g)$ .

Our first observation in case  $e \neq 3^k$  is that  $\pi(g)$  fixes the subset  $\Omega_2 \subseteq W$  r szhalmazt. To see this, notice that if the monomial matrix  $g$  fixes  $y$ , then  $\pi(g)$  permutes the basis elements appearing in  $y$  with zero coefficients between each other. So  $\pi(g)$  fixes both  $\underline{u}_1 \cup \Omega$  and  $\underline{u}_1$  (since  $g$  does), therefore it fixes  $\Omega_2$ . Since  $W = \{\underline{u}_1\} \cup \Omega_2 \cup \Omega_3$  is a  $\pi(C_G(\underline{u}_1))$ -regular partition, we get  $\pi(g) = 1$ . Hence  $g = \delta(g)$  is a diagonal matrix. If  $g_{ii}$  denote the  $i$ -th element of the main diagonal of  $g$ , then  $g \in C_G(y)$  holds only if  $g_{ii} = 1$  for all  $\underline{u}_i \in \Omega_3$ . Since  $e$  is neither 2-power nor 3-power, we can apply Theorem 2.5 and the second part of Corollary 2.2 to get  $|\Omega_2| < \frac{1}{4}e$ . Using part 4 of Lemma 3.4 it follows that  $g = 1$ .

In case of  $e = 3^k$ ,  $k \geq 3$  we see that  $\pi(g)$  fixes the subset  $\Omega_3 \subseteq W$ , since these elements occur with non-zero coefficient 0 in  $y$ . (not counting  $x = \underline{u}_1$  which is already fixed by  $g$ .) However, in this case it is possible that  $\pi(g)$  takes the unique element of  $\Omega_2$  into an element of  $\Omega_4$ . Of course, in that case it takes an element of  $\Omega_4$  into the element of  $\Omega_2$ . This results the appearance of an  $\alpha$  and an  $\alpha^{-1}$  in the main diagonal of  $\delta(g)$ . It follows that the number of  $\neq 1$  elements in the main diagonal of  $\delta(g)$  is at most  $|\Omega_2| + 2$ , which is less than  $\frac{1}{4}e$  by Corollary 2.2, if  $e \neq 9$ . By part 4 of Lemma 3.4 we get  $\delta(g) = 1$ , hence  $\pi(g)$  also fixes the unique element of  $\Omega_2$ , so  $g = \pi(g) = 1$ .

It remains to examine the cases  $e = 9$  and  $e = 3$ . In case of  $e = 9$  we have  $y = \alpha \cdot \underline{u}_i + 0 \cdot \underline{u}_j + 1 \cdot \sum_{k \neq i,j,1} \underline{u}_k$ . Then  $\pi(g)$  fixes  $\underline{u}_j$ . If  $\pi(g)$  fixes also  $\underline{u}_i$ , then  $\pi(g) = 1$ . In this case the only not necessarily 1 element in the main diagonal of  $g = \delta(g)$  is  $g_{jj}$ . Using part 4 of Lemma 3.4 we get  $g = 1$ . If  $\pi(g)$  does not fix  $\underline{u}_i$ , then in the main diagonal of  $\delta(g)$  there are an  $\alpha$  and an  $\alpha^{-1}$ , possibly  $\delta(g)_{jj} \neq 1$ , any other element is 1. Since  $S$  acts regularly on  $W$ , we can choose an element  $s \in S$  which takes the bases element corresponding to  $\alpha^{-1}$  into the bases element corresponding to  $\alpha$ . Then, in the main diagonal of  $[\delta(g), s]$  appear an  $\alpha^2 \neq 1$  and at least four 1's. However, there is no such an element in  $D = A \times D_0$  by part 4 of Theorem 3.3, contradicting to part 3 of Lemma 3.4.

Finally, let  $e = 3$ . If  $g \in C_G(x) \cap C_G(y)$  is diagonal, then clearly  $g = 1$ . Otherwise,

$$\delta(g) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-1} \end{pmatrix} \text{ and } [\delta(g), s] = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^{-2} & 0 \\ 0 & 0 & \alpha \end{pmatrix}, \text{ for } s = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in S.$$

Since  $o(\alpha) \geq 6$  we get  $\alpha \neq \alpha^{-2}$ , so  $[\delta(g), s] \notin D$  by part 4 of Theorem 3.3, which is impossible by part 3 of Lemma 3.4.  $\square$

### 3.2.2 Case $e = 2^t$

Keeping the assumption that  $F$  is monomial, now we handle the case  $e = 2^k$  for some  $k$ . We note that in case of  $e \leq 128$  we could give similar constructions as we did in Theorem 3.5. However, for a more uniform discussion we alter these constructions a bit, so it will be adequate even in smaller dimensions. The point of our modification is that we do not choose  $x$  as a bases element this time, rather as a linear combination of exactly three bases vectors. Although this effects that  $C_G(x)$  will not be monomial any more, but we can cure this problem by a good choice of  $y$ .

In case  $e = 2$  any bases will be obviously good, let for example  $x = \underline{u}_1, y = \underline{u}_2$ . Now, we analyze the case  $e = 4$ . According to Theorem 3.3, we choose a bases  $\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4 \in V$ . Now,  $F = AD_0S$ , where the Klein groups  $D_0 = \langle d_1, d_2 \rangle$  and  $S = \langle s_1, s_2 \rangle$  are generated (independently from the base field) by the matrices:

$$d_1 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix}, d_2 = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix},$$

$$s_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} s_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

We could already observe that the smaller the dimension and the size of the base field the harder to find a good pair of vectors. Therefore, it is not surprising that the most complicated part is to make clear the problem for subgroups of  $G \leq GL(4, 3)$ ,  $G \leq GL(4, 9)$  and  $G \leq GL(4, 5)$ . In the first two case we need to use even the assumption  $(|G|, |V|) = 1$ , while in case of  $GL(4, 5)$  we found a suitable pair of vectors by using a computer. Our next two theorems are about these cases.

**Theorem 3.6.** *Let  $F = A \langle d_1, d_2, s_1, s_2 \rangle \triangleleft G \leq GL(4, 3^k)$ . Furthermore, set  $x_1 = \underline{u}_2 + \underline{u}_3 + \underline{u}_4$ , and  $y_1 = \underline{u}_1$ . Then  $|C_G(x_1) \cap C_G(y_1)| \leq 2$ . If the pair of vectors  $x_1, y_1$  would not be a good choice, then let  $1 \neq g_0 \in C_G(x_1) \cap C_G(y_1)$ . Then  $g_0$  is a permutation matrix fixing one of the elements  $\underline{u}_2, \underline{u}_3, \underline{u}_4$ . We can assume that  $g_0(\underline{u}_2) = \underline{u}_2$ . Let us define the vectors  $x_2, y_2, x_3, y_3 \in V$  as*

$$\begin{aligned} x_2 &= \underline{u}_1 + \underline{u}_2 + \underline{u}_4, & y_2 &= \underline{u}_1 + \underline{u}_3; \\ x_3 &= \underline{u}_1 + \underline{u}_2 - \underline{u}_4, & y_3 &= \underline{u}_1 + \underline{u}_3. \end{aligned}$$

*Now, either  $C_G(x_2) \cap C_G(y_2) = 1$ , or  $C_G(x_3) \cap C_G(y_3) = 1$ .*

*Proof.* We know that  $C_G(y_1)$  consists of monomial matrices by part 1 of Lemma 3.4, so any  $g \in C_G(x_1) \cap C_G(y_1)$  acts as a permutation on the set  $\{\underline{u}_2, \underline{u}_3, \underline{u}_4\}$ . Since the order of  $|G|$  is not divisible by 3, we get  $C_G(x_1) \cap C_g(y_1)$  is isomorphic to a 3'-subgroup of the symmetric group  $S_3$ , so  $|C_G(x_1) \cap C_G(y_1)| \leq 2$ , and the first part of the theorem is proved.

Let us assume that

$$g_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in G.$$

Now,  $C_G(\underline{u}_1 + \underline{u}_3)$  normalizes the subgroup  $N = C_F(\underline{u}_1 + \underline{u}_3)$  generated by the elements  $d_2, s_2$ . It is easy to check that the  $N$ -invariant subspaces

$$\langle \underline{u}_1 + \underline{u}_3 \rangle, \langle \underline{u}_1 - \underline{u}_3 \rangle, \langle \underline{u}_2 + \underline{u}_4 \rangle, \langle \underline{u}_2 - \underline{u}_4 \rangle$$

are pairwise non-equivalent representations of  $N$ . Hence  $C_G(\underline{u}_1 + \underline{u}_3)$  permutes these subspaces. (In other words, it consists of monomial matrices with respect to this new basis.) Of course,  $C_G(\underline{u}_1 + \underline{u}_3)$  fixes the subspace  $\langle \underline{u}_1 + \underline{u}_3 \rangle$ . Using again that  $|G|$  is not divisible by 3, we get at least one of the following holds:

$$\begin{aligned} \forall g \in C_G(\underline{u}_1 + \underline{u}_3) &\Rightarrow g(\underline{u}_1 - \underline{u}_3) = \alpha_g(\underline{u}_1 - \underline{u}_3) \quad \text{for some } \alpha_g \in \mathbb{F}_{p^a}^*, \\ \forall g \in C_G(\underline{u}_1 + \underline{u}_3) &\Rightarrow g(\underline{u}_2 + \underline{u}_4) = \alpha_g(\underline{u}_2 + \underline{u}_4) \quad \text{for some } \alpha_g \in \mathbb{F}_{p^a}^*, \\ \forall g \in C_G(\underline{u}_1 + \underline{u}_3) &\Rightarrow g(\underline{u}_2 - \underline{u}_4) = \alpha_g(\underline{u}_2 - \underline{u}_4) \quad \text{for some } \alpha_g \in \mathbb{F}_{p^a}^*. \end{aligned}$$

In the first case  $C_G(\underline{u}_1 + \underline{u}_3)$  fixes both the  $\langle \underline{u}_1, \underline{u}_3 \rangle$  and the  $\langle \underline{u}_2, \underline{u}_4 \rangle$  subspaces. Thus, if a  $g \in C_G(\underline{u}_1 + \underline{u}_3)$  fixes either  $x_2$  or  $x_3$ , then  $g(\underline{u}_1) = \underline{u}_1$ , and  $g$  is a monomial matrix. Furthermore, either  $g = 1$ , or  $g(\underline{u}_2) = \beta \underline{u}_4$  and  $g(\underline{u}_4) = \gamma \underline{u}_2$  for some  $\beta, \gamma \in \mathbb{F}_{p^a}^*$ . However, in that case the order of  $g_0 g \in G$  is divisible by three, a contradiction. So, in this case we get  $C_G(x_2) \cap C_G(y_2) = C_G(x_3) \cap C_G(y_3) = 1$ .

In the second case we claim that  $C_G(x_2) \cap C_G(y_2) = 1$ . Let  $g \in C_G(x_2) \cap C_G(y_2)$ . If  $g(\underline{u}_1 - \underline{u}_3) = \beta(\underline{u}_1 - \underline{u}_3)$  for some  $\beta \in \mathbb{F}_{p^a}^*$ , then  $g = 1$  by the previous paragraph. Otherwise,  $g(\underline{u}_1 - \underline{u}_3) = \gamma(\underline{u}_2 - \underline{u}_4)$  holds for some  $\gamma \in \mathbb{F}_{p^a}^*$ . Using that  $\frac{1}{2} = -1$  in  $\mathbb{F}_{3^k}$  we get

$$\begin{aligned} g(\underline{u}_1 + \underline{u}_2 + \underline{u}_4) &= \frac{1}{2}(g(\underline{u}_1 + \underline{u}_3) + g(\underline{u}_1 - \underline{u}_3)) + g(\underline{u}_2 + \underline{u}_4) = \\ &= (\underline{u}_1 + \underline{u}_3) + \gamma(\underline{u}_2 - \underline{u}_4) + \alpha_g(\underline{u}_2 + \underline{u}_4) \neq \underline{u}_1 + \underline{u}_2 + \underline{u}_4. \end{aligned}$$

This contradiction shows that  $C_G(x_2) \cap C_G(y_2) = 1$ .

Finally, in the third case the proof of  $C_G(x_3) \cap C_G(y_3) = 1$  is essentially the same as the proof was in the second case.  $\square$

### Remark

In the above example, if we start from the decomposition  $F = AD'_0 S'$ , where  $D'_0 = \langle d_2, s_2 \rangle$  and  $S = \langle d_1, s_1 \rangle$ , then the corresponding bases  $\{\underline{u}'_1, \underline{u}'_2, \underline{u}'_3, \underline{u}'_4\}$  suitable to Theorem 3.3 will be the following

$$\underline{u}'_1 = \underline{u}_1 + \underline{u}_3, \quad \underline{u}'_2 = \underline{u}_1 - \underline{u}_3, \quad \underline{u}'_3 = \underline{u}_2 + \underline{u}_4, \quad \underline{u}'_4 = \underline{u}_2 - \underline{u}_4.$$

Written in this new basis, the vectors  $x_2, y_2, x_3, y_3$  have the following form

$$\begin{aligned} x_2 &= -\underline{u}'_1 - \underline{u}'_2 + \underline{u}'_3, & y_2 &= \underline{u}'_1; \\ x_3 &= -\underline{u}'_1 - \underline{u}'_2 + \underline{u}'_4, & y_3 &= \underline{u}'_1. \end{aligned}$$

Hence in case of  $G \leq GL(4, 3)$  we can assume that there exists a pair  $x, y$  such that  $C_G(x) \cap C_G(y) = 1$ , where  $y = \underline{u}_1$ , and  $x$  is the linear combination of exactly three basis vectors with non-zero coefficients.

In case of  $GL(4, 5)$  we used the GAP system [2] to find suitable  $x$  and  $y$ .

**Theorem 3.7.** *As before, let  $F = A \langle d_1, d_2, s_1, s_2 \rangle \leq GL(4, 5)$ , and let  $N$  denote the normalizer of  $F$  in  $GL(4, 5)$ . Then, for  $x = \underline{u}_1 + \underline{u}_2 + 2\underline{u}_3$ ,  $y = \underline{u}_2 + \underline{u}_3 + 2\underline{u}_4$ , we have  $C_N(x) \cap C_N(y) = 1$ .*

Finally, if the size of the base field is not equal to 3, 5 or 9, then the following theorem guarantees the existence of a good pair of  $x$  and  $y$ .

**Theorem 3.8.** *As in the previous theorems let  $F = A \langle d_1, d_2, s_1, s_2 \rangle \triangleleft G \leq GL(4, p^a)$ , and assume that  $p^a \neq 3, 5, 9$ . Furthermore, let  $\alpha \in \mathbb{F}_{p^a}$  be a generator of the multiplicative group of  $\mathbb{F}_{p^a}$ . Set  $x = \underline{u}_2 + \alpha\underline{u}_3 + \alpha^{-1}\underline{u}_4$ ,  $y = \underline{u}_1$ . Then  $C_G(x) \cap C_G(y) = 1$ .*

*Proof.* Let  $g \in C_G(x) \cap C_G(y)$ . By the choice of  $y$  we know that  $g$  is a monomial matrix. The first element in the main diagonal of  $\delta(g)$  is 1, and the others are from the set  $\{1, \alpha, \alpha^{-1}\alpha^2, \alpha^{-2}\}$ . If  $\delta(g)$  contains an  $\alpha$  or an  $\alpha^{-1}$ , then for some  $s \in S$  we get  $[\delta(g), s] \in A \times D_0$  contains both  $\alpha$  and  $\alpha^{-1}$ . By part 4 of Theorem 3.3, this is impossible unless  $o(\alpha^2) \mid 4$ , which cannot hold by our assumption to  $p^a$ . It follows that either  $g = 1$ , or

$$g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^2 \\ 0 & 0 & \alpha^{-2} & 0 \end{pmatrix}, \quad \text{and} \quad [\delta(g), s_2] = \begin{pmatrix} \alpha^2 & 0 & 0 & 0 \\ 0 & \alpha^{-2} & 0 & 0 \\ 0 & 0 & \alpha^{-2} & 0 \\ 0 & 0 & 0 & \alpha^2 \end{pmatrix}.$$

It follows from  $[\delta(g), s_2] \in D$  that  $o(\alpha^4) \mid 2$ , which is again impossible, since  $p^a \neq 3, 5, 9$ .  $\square$

The constructions given in the last three theorems have the common property that  $x$  is a sum of exactly three basis vectors with non-zero coefficient. Capitalizing this property, we shall give a uniform construction in any case of  $F = AD_0S \triangleleft G \leq GL(2^k, p^a)$  for all  $k \geq 3$ . Possibly taken a permutation of the basis vectors  $\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e$  we can assume that  $\{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4\}$  corresponds to a two dimensional subspace of  $S$ , that is,

$$\{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4\} = S_2(\underline{u}_1) = \{s(\underline{u}_1) \mid s \in S_2\} \quad \text{for some } S_2 \leq S, \quad |S_2| = 4.$$

Let  $V' = \langle \underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4 \rangle \leq V$  the subspace generated by the first four basis vectors, and  $N_F(V')$  the subgroup of elements of  $V'$  fixing  $F$ . Now,  $N_F(V')/C_F(V')$  is included into  $GL(V')$  by restriction to  $V'$ , so we get a subgroup  $F' = A \langle d_1, d_2, s_1, s_2 \rangle \leq GL(V')$ . If  $g \in N_G(V')$ , then it is clear that  $g_{V'}$  normalizes  $F'$ -t. Using the previous results, we can define  $x_0, y_0 \in V'$  such that  $x_0$  is the linear combination of exactly three basis vectors and  $N_G(V') \cap C_G(x_0) \cap C_G(y_0)$  acts trivially on  $V'$ . Starting from the pair  $x_0, y_0$ , we search a good pair of vectors  $x, y \in V$  in the form  $x = x_0$ ,  $y = y_0 + v$ , where  $v \in V'' := \langle \underline{u}_5, \underline{u}_6, \dots, \underline{u}_e \rangle$ . The following lemma answers the question why this form is good.

**Lemma 3.9.**  $C_G(x_0)$  fixes both the  $V'$  and the  $V''$  subspaces, that is,  $C_G(x_0) \leq N_G(V') \cap N_G(V'')$ . As a result, for any  $v \in V''$  we have  $C_G(x_0) \cap C_G(y_0 + v) = C_G(x_0) \cap C_G(y_0) \cap C_G(v)$  acts trivially on  $V'$ . In particular,  $C_G(x_0) \cap C_G(y_0 + v)$  consists of monomial matrices.

*Proof.* It is enough to prove the inclusion  $C_G(x_0) \leq N_G(V') \cap N_G(V'')$ , the rest of the statement follows evidently. Our proof is similar to how we have proved that  $C_G(\underline{u}_1)$  consists of monomial matrices. As there occurs three basis element in  $x_0$  and  $S \simeq Z_2^{e_1}$  permutes regularly the basis element we get  $C_F(x_0) \leq AD_0$ , i.e., every element of  $C_F(x_0)$  is diagonal. Hence every element of  $C_F(x_0)$  fixes the three basis element appearing in  $x_0$ . Using the assumption that  $\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4$  corresponds to the subspace  $S_2 \leq S$ , it follows easily that any element of  $D_0$  fixing three of the basis elements  $\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4$  must fix the fourth one, too. From our choice  $D_0 = C_D(\underline{u}_1)$  (see proof of Theorem 3.3)  $N := C_F(x_0) = C_{D_0}(S_2)$ . It is clear from this that  $C_{D_0}(S_2)$  is a two codimensional subspace of  $D_0$ -nak, so  $V'$  is just  $N$  the homogeneous component of  $N$  corresponding to the trivial representation, while  $V''$  is the sum of all of the other homogeneous component of  $N$ . (These homogeneous components corresponds to cosets of  $S_2$  in  $S$ .) As  $N \triangleleft C_G(x_0)$ , we get every element of  $C_G(x_0)$  permutes the homogeneous components of  $N$ . Since  $x_0 \in V'$ , we get  $C_G(x_0)$  fixes  $V'$ , so it also fixes the sum of the other components, which is  $V''$ .  $\square$

It is time to define the vector  $v$ , whereby we close the monomial case. We already know from the previous lemma that  $C_G(x_0) \cap C_G(y_0 + v)$  consists of monomial matrices for any  $v \in V''$ , so we can use the constructions given in Theorem 2.1 to define a  $\pi(C_G(x_0) \cap C_G(y_0))$ -regular partition on the space  $W = \{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e\}$ .

**Theorem 3.10.** By part 2.1 of Theorem 5-6 let  $W = \Omega_1 \cup \Omega_2 \cup \dots \cup \Omega_5$  be a  $\pi(C_G(x_0) \cap C_G(y_0))$ -regular partition of  $W = \{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_e\}$  such that  $\Omega_1 = \{\underline{u}_1\} \cup \Omega_2 \cup \Omega_3 \leq \{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4\}$ . (We can achieve this by choosing a suitable  $S$ .) Let the vectors  $x, y \in V$  be defined as follows

$$x = x_0, \quad y = y_0 + v, \quad \text{where } v = 0 \cdot \sum_{\underline{u}_i \in \Omega_4} \underline{u}_i + 1 \cdot \sum_{\underline{u}_i \in \Omega_5} \underline{u}_i, \quad \text{for } e \neq 16.$$

In case of  $e = 16$  this construction is not effective (since it was an exceptional case in Corollary 2.2). In this case let  $\underline{u}_s, \underline{u}_t \in \{\underline{u}_5, \underline{u}_6, \dots, \underline{u}_{16}\}$  be two vectors corresponding to elements from different cosets of  $S_2$  in  $S$ . In this case let  $x, y \in V$  be chosen as

$$x = x_0, \quad y = y_0 + 0 \cdot \underline{u}_s + (-1) \cdot \underline{u}_t + 1 \cdot \sum_{\substack{i \in \{5, 6, \dots, 16\} \\ i \neq s, t}} \underline{u}_i.$$

The we have  $C_G(x) \cap C_G(y) = 1$ .

*Proof.* We know by the previous lemma that any  $g \in C_G(x) \cap C_G(y)$  is a monomial matrix fixing all the vectors  $\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4$ , so it fixes all of the sets  $\Omega_1, \Omega_2, \Omega_3$ . In case  $e \neq 16$  even  $\Omega_4$  is fixed by  $\pi(g)$ , since exactly the element from  $\Omega_4$  are colored by 0. It follows that  $\pi(g) = 1$ . Hence  $g = \delta(g)$  is a diagonal

matrix, and any element in its main diagonal not corresponding to  $\Omega_4$  must be 1. However,  $|\Omega_4| < 1/4|W|$  by Corollary 2.2, so we get  $g = \delta(g) = 1$  by part 4 of Lemma 3.4.

In case  $e = 16$  for the permutation part of any element  $g \in C_G(x) \cap C_G(y)$  we have  $\pi(g)(\underline{u}_s) = \underline{u}_s$ . Now, if  $\pi(g)(\underline{u}_t) \neq \underline{u}_t$  does not hold, then the number of elements in the diagonal of  $\delta(g)$  different from 1 should be 2 or 3, which is again a contradiction to part 4 of Lemma 3.4. Hence  $\delta(g) = 1$  and  $\pi(g)(\underline{u}_t) = \underline{u}_t$ . By choice of the vectors  $\underline{u}_s, \underline{u}_t$  we get  $g = \pi(g) = 1$ , which proves the identity  $C_G(x) \cap C_G(y) = 1$ .  $\square$

### 3.3 Finding $x, y \in V$ in case $F$ is not monomial

Now, we handle the case when  $F$  is not monomial. Thus, the extraspecial 2-group, say  $P_1$ , in the decomposition of  $F \triangleleft G \leq GL(V) \simeq GL(e, p^a)$  corresponding to part 4 of Theorem 3.1 is the central product of a quaternion group  $Q$  by some (maybe 0) dieder groups  $D_4$ . If  $\lambda \in A$  is a field element of order four, and  $Q = \langle i, j \rangle \leq P_1$  is the quaternion group generated by the element  $i, j$  of order four, then defining  $H = \langle \lambda i, \lambda j \rangle \leq AQ$  we get  $H \simeq D_4$  and  $AH = AQ$ . These means that in the decomposition of  $F$  we can exchange  $Q$  for a subgroup isomorphic to  $D_4$ , so we get the monomial case. Therefore, we can assume that  $A$  does not contain a fourth root of unity. Our next theorem is analogous to Theorem 3.3.

**Theorem 3.11.** *With the above assumptions, the subgroup  $F \leq GL(V)$  has the following properties*

1. *There exists a (not necessarily direct) product decomposition  $F = QF_1$  such that  $F_1 = C_F(Q) = D \rtimes S = (A \times D_0) \rtimes S$  and*

$$D_0 \simeq S \simeq Z_2^{e_1-1} \times Z_{p_2}^{e_2} \times \dots \times Z_{p_k}^{e_k}.$$

2. *There is a basis  $\underline{u}_1, \underline{v}_1, \underline{u}_2, \underline{v}_2, \dots, \underline{u}_{e/2}, \underline{v}_{e/2} \in V$  such that written in this basis the elements of  $D$  are diagonal matrices, while  $S$  permutes the set of ordered pairs  $\{(\underline{u}_i, \underline{v}_i) \mid 1 \leq i \leq e/2\}$  regularly.*
3. *The subspaces  $\langle \underline{u}_i \rangle$  are all the irreducible representations of  $D_0$  over  $\mathbb{F}_{p^a}$  and they are pairwise non-equivalent.*
4. *For any  $g \in D_0$ , the main diagonal of  $g$  contains all of the  $o(g)$ -th root of unity with the same multiplicity.*
5. *For all  $1 \leq i \leq e/2$  any element of  $D$  restricting to  $W_i = \langle \underline{u}_i, \underline{v}_i \rangle$  is a scalar matrix.*
6. *If an element  $g \in QD$  has an eigenvalue (in this representation), then  $g \in D$ .*

*Proof.* If  $P_1 = QT$  is the central product of the quaternion group  $Q$  and the extraspecial 2-group  $T$  (which is itself a central product of some  $D_4$ 's), then we can apply Theorem 3.3 to the group  $F_1 = ATP_2P_3 \dots P_k$ . Hence the first statement follows at once from part 1 of Theorem 3.3.

Let  $V_1 \leq V$  be an irreducible  $F_1$ -invariant subspace of  $V$ . By Theorem 3.3 the dimension of  $V_1$  is  $e/2$ , furthermore, there exists a basis  $\{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_{e/2}\} \in V_1$



of  $V_1$  such that  $D$  consists of diagonal matrices respect to this basis, while  $S$  permutes regularly the elements of this basis. Now, statement 3 is just the redefinition of the corresponding part of Theorem 3.3.

Let  $W_i = \langle q(\underline{u}_i) \mid q \in Q \rangle$  be the smallest  $Q$ -invariant subspace containing  $\underline{u}_i$ . Then each  $W_i$  is a homogeneous  $D_0$ -module, since  $Q$  centralizes  $D_0$ , so 5 follows. Additionally, these subspaces are pairwise non-equivalent  $D_0$ -modules.

Since  $Q$  centralizes also  $S$ , we get  $S$  permutes regularly the subspaces  $W_i$ . It follows that  $W_1 \oplus W_2 \oplus \dots \oplus W_{e/2}$  is an  $F$ -invariant subspace, so it is equal to  $V$  by part 7 of Theorem 3.1. Comparing dimensions we get each  $W_i$  is two dimensional. Let us choose elements  $\underline{v}_i \in W_i$  such that  $\underline{u}_i, \underline{v}_i$  is a basis of  $W_i$  for all  $i$ , and the set of vectors  $\{\underline{v}_1, \underline{v}_2, \dots, \underline{v}_{e/2}\}$  is an orbit of  $S$ . Now, 2 follows obviously.

Using the corresponding part of the monomial case it follows 4 at once.

Finally, let  $g = qd \in QD \setminus D$ , so  $q \in Q \setminus \{\pm I\}$ . As the elements of  $Q$  are commutable with the elements of  $D$  and the exponent of  $D$  is not divisible by 4 (Here we use that  $A$  does not contain a fourth root of unity), we get the order of  $g$  is divisible by four. It follows that  $g^{o(g)/2}$  is an element of  $Q$  of order two, hence  $g^{o(g)/2} = -I$ . Now, if  $\lambda$  is an eigenvalue of  $g$ , then  $\lambda^{o(g)/4} \in \mathbb{F}_{p^a}$  would be a fourth root of unity, a contradiction. Hence any element of  $QD \setminus D$  does not have an eigenvalue, which proves 6.  $\square$

According to the last theorem let  $V_1 = \langle \underline{u}_1, \underline{u}_2, \dots, \underline{u}_e \rangle$  and  $V_2 = \langle \underline{v}_1, \underline{v}_2, \dots, \underline{v}_e \rangle$ . Then  $V = V_1 \oplus V_2$ . Let  $N_G(V_1)$  denote the elements of  $G$  fixing the subspace  $V_1$ . Then the restriction of  $G_1 = N_G(V_1)/C_G(V_1)$  to  $V_1$  gives us an inclusion  $G_1 \leq GL(V_1)$ . It is clear that  $G_1$  contains the restriction of  $F_1$  to  $V_1$  as a normal subgroup. Using the constructions of the monomial case, we can find vectors  $x_1, y_1 \in V_1$  such that  $C_{G_1}(x_1) \cap C_{G_1}(y_1) = 1_{V_1}$ . Furthermore, in cases  $e/2 \neq 2^t$  and  $e/2 = 2$  we have  $x_1 = \underline{u}_1$  by Theorem 3.5, while in cases  $e/2 = 2^t$ ,  $t \geq 2$  we found  $x_1 \in \langle \underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4 \rangle$  as a linear combination of exactly three basis vectors, while  $y \in \underline{u}_1 + \langle \underline{u}_5, \underline{u}_6, \dots, \underline{u}_{e/2} \rangle$ . (Theorems 3.6-3.8, 3.10, and Remark after Theorem 3.6) Starting from these constructions we define vectors  $x, y \in V$  as follows.

**Theorem 3.12.** *Using the vectors  $x_1, y_1 \in V_1$  defined above let*

$$\begin{aligned} x &= x_1, & y &= \underline{v}_1 + y_1, & \text{in cases } e/2 \neq 2^k \text{ or } e/2 = 2; \\ x &= \underline{u}_1 + x_1, & y &= y_1, & \text{in cases } e/2 = 2^k, k \geq 2. \end{aligned}$$

Then  $C_G(x) \cap C_G(y) = 1$ .

*Proof.* First, let  $e/2 \neq 2^k$  or  $e/2 = 2$ . Choosing a  $g \in C_G(x) \cap C_G(y)$  it normalizes the subgroup  $C_F(x) = C_F(\underline{u}_1) = D_0$ , so it permutes the homogeneous components of  $D_0$ , that is, the subspaces  $W_1, W_2, \dots, W_{e/2}$ . Then it is clear from the construction of  $y$  that  $g$  also centralizes  $\underline{v}_1$ , so the restriction of  $g$  to  $W_1$  is the identity. As  $g$  permutes the subspaces  $W_1, W_2, \dots, W_{e/2}$  it follows that  $g$  can be written in a unique way as a product  $g = \delta_2(g)\pi_2(g)$ , where  $\delta_2(g)$  is a 2-block diagonal matrix, while  $\pi_2(g) = \pi(g) \otimes I_2$ , where  $\pi(g)$  denotes the permutation action of  $g$  on the set  $\{W_1, W_2, \dots, W_{e/2}\}$ . Similarly to part 3 of Lemma (3.4) one can prove that  $\delta_2(g)$  must normalize  $F$ , as well. Now, if  $\underline{u}_i$  appears with a non-zero coefficient in  $y$ , then the  $i$ -th block of  $\delta_2(g)$  must be a upper triangular matrix. If we choose  $s \in S$  such that  $s(\underline{u}_1) = \underline{u}_i$ , then the first

block of the 2-block diagonal matrix  $[\delta_2(g), s] \in QD$  is the same as the  $i$ -th block of  $\delta_2(g)$ . As a upper triangular matrix does have an eigenvalue, by part 6 of Theorem 3.11 we get  $[\delta_2(g), s] \in D$ , so every block of  $[\delta_2(g), s]$ , in particular, the first one, is scalar matrix. Thus, we showed that for any  $\underline{u}_i$  appearing in  $y$  the corresponding block of  $\delta_2(g)$  is scalar matrix. Such  $\underline{u}_i$ 's are in bijection with the elements of some  $\Omega_i$ 's in Theorems 2.1 and 2.5. (see also Theorem 3.5) It is easy to check that in any such case more than half of the  $\underline{u}_i$ 's appears in  $y$ , so more than half of the blocks of  $\delta_2(g)$  is scalar matrix. It follows that for any  $s \in S$  at least one block of  $[\delta_2(g), s] \in QD$  is a scalar matrix. Using part 6 of Theorem 3.11 again, we get  $[\delta_2(g), s]$  is diagonal matrix for all  $s \in S$ . Since the first block of  $\delta_2(g)$  is the identity, and  $S$  regularly permutes the blocks we get every block of  $\delta_2(g)$  is scalar matrix, that is,  $\delta_2(g)$  is diagonal. Hence  $g$  is monomial, and it fixes the subspace  $V_1 = \langle \underline{u}_1, \underline{u}_2, \dots, \underline{u}_{e/2} \rangle$ . As  $g_{V_1} \in C_{G_1}(x_1) \cap C_{G_1}(y_1) = 1_{V_1}$ , we have  $g$  acts on  $V_1$  trivially, so  $\pi(g) = 1$ , and  $g$  is a diagonal matrix. Finally, using that the restriction of  $g$  to any  $W_i$  is a scalar matrix, and  $g(\underline{u}_i) = \underline{u}_i$  for all  $i$  it follows that  $g = 1$ , what we wanted to prove.

In case  $e = 2^k$ ,  $k \geq 2$  we claim that  $C_F(x) = C_F(\underline{v}_1) \cap C_F(x_1) \leq D_0$ . As the set of subspaces  $W_1, W_2, W_3, W_4$  corresponds to a subspace of  $S$ , it follows that  $C_F(x)$  permutes these subspaces. Now, if  $g \in C_F(x)$  takes  $\underline{u}_i$  into a multiple of  $\underline{u}_j$  for some  $\underline{u}_i, \underline{u}_j$  occurring in  $x$ , then  $\underline{u}_j$  is an eigenvalue of the 2-block diagonal part  $\delta_2(g) \in QD$  of  $g$ , hence  $\delta_2(g)$  is diagonal by part 6 of Theorem 3.11. Consequently,  $g$  cannot take  $\underline{v}_1$  into a multiple of some  $\underline{u}_i$ . So  $C_F(x)$  fixes both  $\underline{v}_1$  and  $x_1$ , which proves that  $C_F(x) = C_F(\underline{v}_1) \cap C_F(x_1) \leq D_0$ .

It follows that the homogeneous component corresponding to the trivial representation of  $C_F(x) \leq D_0$  is just the subspace  $W_1 \oplus W_2 \oplus W_3 \oplus W_4$ , while the subspace generated by the other homogeneous components of  $C_F(x)$  is  $W_5 \oplus W_6 \oplus \dots \oplus W_{e/2}$ . Since any  $g \in C_G(x) \cap C_G(y)$  normalizes  $C_F(x)$ , it permutes these homogeneous components. We get  $g$  fixes both  $W_1 \oplus W_2 \oplus W_3 \oplus W_4$  and  $W_5 \oplus W_6 \oplus \dots \oplus W_{e/2}$ . As  $y$  is of the form  $y = \underline{u}_1 + \langle \underline{u}_5, \underline{u}_6, \dots, \underline{u}_{e/2} \rangle$ , it follows that  $g(\underline{u}_1) = \underline{u}_1$ , so  $g$  fixes the subspace  $W_1$ , and permutes the subspaces  $W_2, \dots, W_{e/2}$ . Using the construction of  $x$  we get  $g(\underline{v}_1) = \underline{v}_1$ , so  $g$  acts trivially on  $W_1$ . From this point our proof is the same as it was for the previous case.  $\square$

## 4 Imprimitve linear groups

As before, let  $p \neq 2$  prime (or prime power), let  $V$  be a finite vector space over  $\mathbb{F}_p$  and  $G \leq GL(V) \simeq GL(n, p)$  solvable linear group such that  $(|G|, |V|) = 1$ . In case of  $G$  is a primitive linear group, the previous section gave us a base  $x, y \in V$ . Using this result, in this section we handle the case, when  $G$  is not primitive as a linear group.

It follows from Maschke's theorem that  $V$  is an completely reducible  $G$ -module. The next obvious lemma reduce the problem to irreducible  $G$ -modules.

**Lemma 4.1.** *Let  $V = V_1 \oplus V_2$  the sum of two  $G$ -invariant subspaces. Now,  $G/C_G(V_i) \leq GL(V_i)$  acts faithfully on  $V_i$ . For  $i = 1, 2$ , set  $x_i, y_i \in V_i$  such that  $C_G(x_i) \cap C_G(y_i) = C_G(V_i)$ . Then  $C_G(x_1 + x_2) \cap C_G(y_1 + y_2) = 1$ .*

Let  $G \leq GL(V)$  be an irreducible, imprimitive linear group. Thus, there is a decomposition  $V = \oplus_{i=1}^k V_i$  such that  $k \geq 2$  and  $G$  permutes the subspaces  $V_i$  in a transitive way. We can assume that the decomposition cannot be refined. For

each  $1 \leq i \leq k$  let  $H_i = \{g \in G \mid gV_i = V_i\}$  be the stabilizer of  $V_i$  in  $G$ . Then  $H_i/C_{H_i}(V_i) \leq GL(V_i)$  is a linear group, and the subgroups  $H_i$  are conjugate in  $G$ . Of course,  $(|H_1|, |V_1|) = 1$ , so, using the previous section we can find vectors  $x_1, y_1 \in V_1$  such that  $C_{H_1}(x_1) \cap C_{H_1}(y_1) = C_{H_1}(V_1)$ . Let  $\{g_1 = 1, g_2, \dots, g_k\}$  be a set of right coset representatives to  $H_1$  in  $G$  such that  $V_i = g_i V_1$  for all  $1 \leq i \leq k$ , and let  $x_i = g_i x_1$ ,  $y_i = g_i y_1$ . It is clear that  $H_i = H_1^{g_i^{-1}}$  and  $C_{H_i}(x_i) \cap C_{H_i}(y_i) = C_{H_i}(V_i)$ .

Now,  $N = \cap_{i=1}^k H_i$  is a normal subgroup of  $G$ , the quotient group  $G/N$  acts faithfully and transitively on the set  $\{V_1, V_2, \dots, V_k\}$ , and  $|G/N|$  is coprime to  $p$ . Using Theorem 2.3, we can choose a vector  $(a_1, a_2, \dots, a_k) \in \mathbb{F}_p^k$  such that (to the above permutation action) only the identity element of  $G/N$  fixes this vector.

**Theorem 4.2.** *Let the vectors  $x, y \in V$  be defined as*

$$x = \sum_{i=1}^k x_i, \quad y = \sum_{i=1}^k (y_i + a_i x_i).$$

*Then  $C_G(x) \cap C_G(y) = 1$ .*

*Proof.* Let  $g \in C_G(x) \cap C_G(y)$ . Assuming that  $gV_i = V_j$  for some  $1 \leq i, j \leq k$  we get  $gx_i = x_j$  and  $g(y_i + a_i x_i) = (y_j + a_j x_j)$ . Choose  $g' = g_j^{-1} g g_i \in G$ . Ekkor

$$g'x_1 = x_1 \quad \text{and} \quad g'(y_1 + a_i x_1) = (y_1 + a_i x_1) + (a_j - a_i)x_1, \quad (2)$$

so  $g'$  stabilizes the subspace  $\langle x_1, y_1 \rangle \leq V_1$ . If  $y_1 = cx_1$  for some  $c \in \mathbb{F}_p$ , then  $g'y_1 = y_1$ . Using the identity (2) we get  $a_j = a_i$ . Otherwise,  $x_1, y_1 + a_i x_1$  form a basis of the subspace  $\langle x_1, y_1 \rangle$  which is a two dimensional  $g'$ -invariant subspace. With respect to the basis  $x_1, y_1 + a_i x_1$ , the restriction of  $g'$  to this subspace has matrix form

$$\begin{pmatrix} 1 & a_j - a_i \\ 0 & 1 \end{pmatrix}.$$

If  $a_j - a_i \neq 0$ , then this matrix has order  $p$ , so  $p$  divides the order of  $g' \in G$ , a contradiction. Hence in any case  $a_i = a_j$  holds for  $gV_i = V_j$ , which exactly means that  $gN \in G/N$  stabilizes the vector  $(a_1, a_2, \dots, a_k)$ . It follows that  $g \in N$ . So  $gx_i = x_i$  and  $gy_i = y_i$  holds for any  $1 \leq i \leq k$ , and  $g \in \cap_{i=1}^k C_{H_i}(V_i) = C_G(V) = 1$  follows.  $\square$

## References

- [1] S. Dolfi, Intersections of odd order Hall subgroups, Bull. London Math. Soc. **37** (2005) 67–74.
- [2] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; 2002 (<http://www.gap-system.org>)
- [3] D. Gluck, Trivial set-stabilizers in finite permutation groups, Canad. J. Math. **35** (1983), 59–??.
- [4] D. Gluck and K. Magaard, Base sizes and regular orbits for coprime affine permutation groups, J. London Math. Soc. (2) **58** (1998), 603–618.

- [5] B. Hartley and A. Turull, On characters of coprime operator groups and the Glaubermann character correspondence, *J. Reine Angew. Math.* **451** (1994), 175–219.
- [6] I. M. Isaacs, Large orbits in actions of nilpotent groups, *Proc. Amer. Math. Soc.* **127** (1999) 45–50.
- [7] H. Matsuyama, Another proof of Gluck’s theorem, *J. Algebra* **247** (2002) 703–706.
- [8] A. Moreto and T. Wolf, Orbit sizes, character degrees and Sylow subgroups, *Adv. Math.* **184** (2004) 18–36.
- [9] P. P. Pálffy, Bounds for linear groups of odd order, *Proc. Second Internat. Group Theory Conf., Bressanone/Brixen 1989*, *Suppl. Rend. Circ. Mat. Palermo* **23** (1990) 253–263.
- [10] L. Pyber, ‘Asymptotic results for permutation groups’, *Groups and computation*, DIMACS Ser. Discrete Math. Theoret. Comp. Sci. 11 (ed. L. Finkelstein and W. Kantor, Amer. Math. Soc., Providence, RI, 1993) 197–219.
- [11] Á. Seress, The minimal base size of primitive solvable permutation groups, *J. London Math. Soc.* **53** (1996) 243–255.
- [12] D. A. Suprunenko, *Matrix groups*, Amer. Math. Soc., Providence, RI, 1976.
- [13] T. Wolf, Large orbits of supersolvable linear groups, *J. Algebra* **215** (1999) 235–247.

Zoltán Halasi  
 Central European University  
 Department of Mathematics  
 and Its Applications  
 H-1051 Budapest  
 Nádor utca 9.  
 Hungary  
 e-mail: haca@cs.elte.hu

Károly Podoski  
 Alfréd Rényi Institute of Mathematics  
 Hungarian Academy of Sciences  
 H-1364 Budapest  
 P. O. Box 127  
 Hungary  
 e-mail: pcharles@cs.elte.hu